UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,494	07/06/2001	Michael Freed	1014-064US01/JNP-0261	4136

72689 7590 04/21/2010

SHUMAKER & SIEFFERT, P.A
1625 RADIO DRIVE , SUITE 300
WOODBURY, MN 55125

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
04/21/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

pairdocketing@ssiplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MICHAEL FREED and ELANGO GANESEN

Appeal 2009-003122
Application 09/900,494
Technology Center 2400

Decided: April 19, 2010

Before: JOHN A. JEFFERY, LANCE LEONARD BARRY, and THU ANN DANG, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

The Patent Examiner rejected claims 1-28. The Appellants appeal therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

INVENTION

The Appellants describe the invention at issue on appeal as follows.

> The present invention provides a unique system and method for implementing SSL [i.e., Secure Sockets Layer] acceleration, and indeed any encryption or decryption methodology, to offload to the computational overhead required with the methodology from a server or client. The invention is particularly suited to offloading encryption and decryption tasks from a server which is normally required to handle a multitude of concurrent sessions. The system may include an SSL acceleration device, which operates to intercept secure communications between, for example, a Web based Internet client such as a Web browser operating on a personal computer, and a Web server. The SSL acceleration device will intercept communications directed to the server and act as a proxy in various embodiments of the invention.

(Spec. 9.)

ILLUSTRATIVE CLAIM

1. A load balancing acceleration device, comprising:

a processor, memory and communications interface;

a TCP communications manager capable of interacting with a plurality of client devices and server devices simultaneously via the communications interface;

a secure communications manager to negotiate a secure communication session with one of the client devices;

an encryption and decryption engine instructing the processor to decrypt data received via the secure communication session and direct the decrypted data to one of said server devices via a second communication session; and

> a load balancing engine associating each of said client devices with a respective one of said server devices based on calculated processing loads of each said server devices,
>
> wherein the decryption engine and the load balancing engine bypass an application layer of a network stack by decrypting the data from the secure communication sessions of the clients and outputting the decrypted data to the associated server devices without processing the data with the application layer of the network stack.

PRIOR ART

Gelman	6,415,329 B1	Jul. 2, 2002
Toporek	6,654,344 B1	Nov. 25, 2003
Abjanic	6,732,175 B1	May 4, 2004
Baskey	6,732,269 B1	May 4, 2004
Hankinson	6,799,202 B1	Sep. 28, 2004

REJECTIONS

Claims 1-28 are rejected under 35 U.S.C. § 112, first paragraph, as lacking an adequate written description.[1]

Claims 1-7 and 22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Hankinson and Toporek.

---

[1] Although the Examiner's statement of the rejection uses the phrase "as failing to comply with the enablement requirement" (Answer 3), his explanation of the rejection, e.g., that "the claim[s] ha[ve] been amended to include the limitation" (*id.*) and that "[t]here is no support for this limitation in the specification" (*id.* at 3-4), makes it clear that the rejection is based on lack of an adequate written description.

Claims 8-11 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Hankinson, Toporek, and Gelman.

Claims 12-15, 17-21, 23 and 24 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Abjanic and Toporek.

Claim 16 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Abjanic, Toporek, and Gelman.

Claims 25-28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Baskey and Toporek.

WRITTEN DESCRIPTION REJECTION

The Examiner makes the following findings.

> Regarding independent claim 1, the claim has been amended to include the limitation "wherein the decryption engine and the load balancing engine bypass an application layer of a network stack by decrypting the data from the secure communication sessions of the clients and outputting the decrypted data to the associated server devices without processing the data with the application layer of the network stack". There is no support for this limitation in the specification.
>
> . . .
>
> Regarding independent claims 12 and 25, both the claims have been amended to include the limitation "without processing the data packets with an application layer of a network stack". There is no support for this limitation in the specification.

(Ans. 3-4.) The "Appellants direct the Board's attention to the network stack shown in the SSL accelerator of Figure 3 . . . ." (App. Br. 13.)

ISSUE

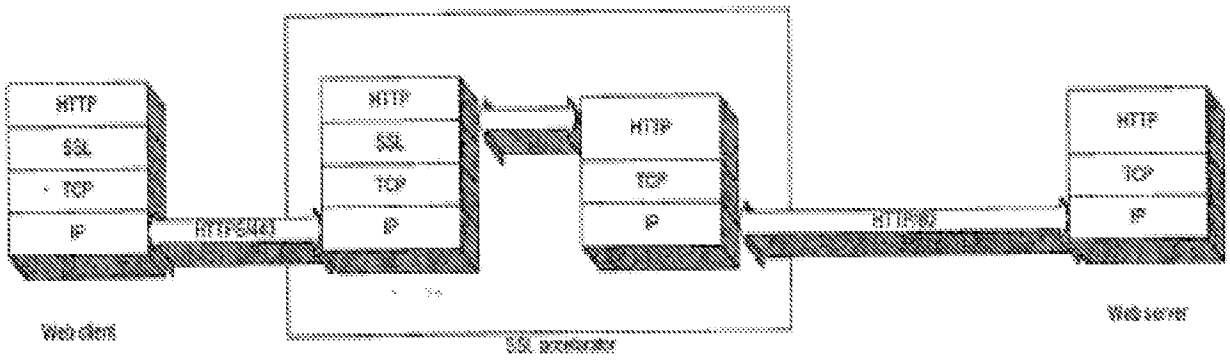
Therefore, the issue before us is whether the Appellants have shown error in the Examiner's finding that the originally filed written description fails to reasonably convey to the artisan that the Appellants had possession at that time of the later claimed subject matter.

LAW

"[T]he test for sufficiency of support . . . is whether the disclosure of the application relied upon 'reasonably conveys to the artisan that the inventor had possession at that time of the later claimed subject matter.'" *Ralston Purina Co. v. Far-Mar-Co., Inc.*, 772 F.2d 1570, 1575 (Fed. Cir. 1985) (quoting *In re Kaslow*, 707 F.2d 1366, 1375 (Fed. Cir. 1983)).

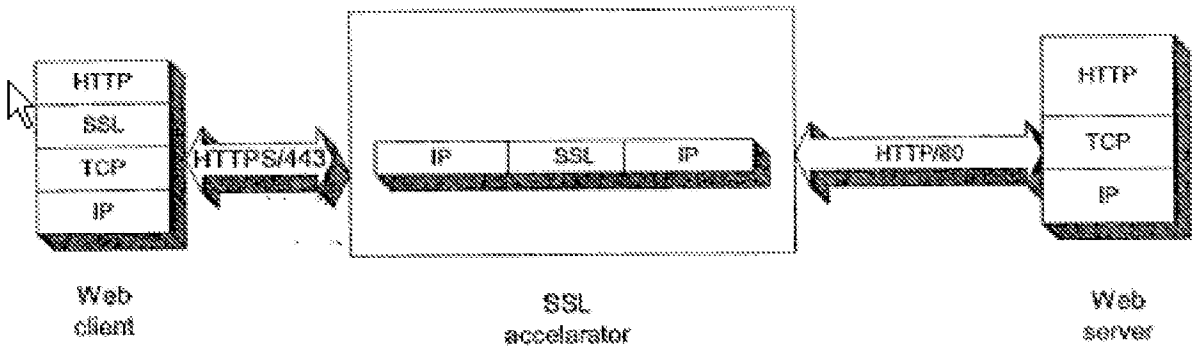
FINDINGS OF FACT ("FFS")

The Appellants' Figure 2B, which was part of their original disclosure, follows.



More specifically "Figure 2B is a block diagram illustrating the computational exercise of SSL accelerator [in] accordance with the prior art." (Spec. 8.)

The Appellants' Figure 3, which was also part of their original disclosure, follows.



More specifically, "Figure 3 shows how the system of the [Appellants'] invention differs in general from that of the prior art, and illustrates the manner in which the SSL encryption and decryption proxy is implemented." (*Id.* at 10.)

ANALYSIS

We agree with the Appellants that in "the network stack shown in the SSL accelerator of Figure 3 . . . , in contrast to the prior art device of Figure 2B, the application layer (e.g., the HTTP [i.e., HyperText Transfer Protocol] protocol) of the network stack is noticeably absent when compared with the prior art accelerator shown in Figure 2B." (Appeal Br. 13.) We further agree with their following argument.

> Figure 3 clearly shows that . . . Appellants' SSL accelerator does not process the secure data received from the web client at the application layer (e.g., HTTP) prior to forwarding the packets to the web server. Rather, . . . the accelerator shown in Figure 3 intercepts data destined for the web server and, rather than the transmitting packets up and down the TCP/IP [i.e., Transmission Control Protocol/Internet Protocol] stack as shown in Figure 2B, will perform the SSL encryption and decryption at the packet level before forwarding the packet on to its destination.

(*Id.*) Emphasis original.

CONCLUSION

Based on the aforementioned facts and analysis, we conclude that the Appellants have shown error in the Examiner's finding that the originally filed written description fails to reasonably convey to the artisan that the Appellants had possession at that time of the later claimed subject matter.

OBVIOUSNESS REJECTIONS

Based on the Appellants' arguments, we will decide the appeal of claims 1-11 and 22; 12-21, 23, and 24; and 25-28 based on the independent claims 1, 12, and 25 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

The Examiner makes the following admissions.

> Hankinson et al does not teach that the decryption engine and the load balancing engine bypass an application layer of a network stack by decrypting the data from the secure communication sessions of the clients and outputting the decrypted data to the associated server devices without processing the data with the application layer of the network stack.

(Ans. 6.) "Abjanic does not teach without processing the data packets with an application layer of a network stack." (*Id* at 9.) "Baskey et al does not teach without processing the data packets with an application layer of a network stack." (*Id.* at 12.) Finding that "Toporek et al teaches bypassing an application layer of a network stack [column 11, lines 22-33]" (*id.* at 6, 9, and 12), however, he concludes that it would have been obvious to modify Hankinson, Abjanic, and Baskey to bypass an application layer of a network stack without processing the reference's data within the application layer of the network stack "because it allows the network layer to communicate directly with the physical layer [column 11, lines 22- 33]." (*Id.*) The Appellants argue that "the combination of references still provides no teaching as to how the application-layer (which is above both the network layer and the physical layer) could be avoided for functions . . . that traditionally require the application-layer." (App. Br. 18.)

ISSUE

Therefore, the issue before us is whether the Appellants have shown error in the Examiner's combining of teachings from Toporek with those of Hankinson, Abjanic, and Baskey.

LAW

The presence or absence of a reason "to combine references in an obviousness determination is a pure question of fact." *In re Gartside*, 203 F.3d 1305, 1316 (Fed. Cir. 2000). "A rejection based on section 103 clearly must rest on a factual basis. . . ." *In re Warner*, 379 F.2d 1011, 1017 (CCPA 1967). "The Patent Office has the initial duty of supplying the factual basis for its rejection. It may not . . . resort to speculation, unfounded assumptions

or hindsight reconstruction to supply deficiencies in its factual basis." (*Id.*) "It is impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious." *In re Fritch*, 972 F.2d 1260, 1266 (Fed. Cir. 1992) (citing *In re Gorman*, 933 F.2d 982, 987 (Fed. Cir. 1991)). Furthermore, the U.S. Court of Appeals for the Federal Circuit "has previously found a proposed modification inappropriate for an obviousness inquiry when the modification rendered the prior art reference inoperable for its intended purpose." *Fritch*, 972 F.2d at 1266 n.12 (citing *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984)). A reason to combine teachings from the prior art, however, "may be found in explicit or implicit teachings within the references themselves, from the ordinary knowledge of those skilled in the art, or from the nature of the problem to be solved." *WMS Gaming Inc. v. Int'l Game Tech.*, 184 F.3d 1339, 1355 (Fed. Cir. 1999) (citing *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

FINDINGS OF FACT

Hankinson teaches that "[a] server implementing the Federated OS [i.e., operating system] can be scaled up to handle . . . encryption/decryption (for example, secure sockets layer (SSL) transactions used for e-commerce) . . ." (Col. 3, ll. 16-19.)

In Abjanic "[a] network apparatus is provided between a network and a plurality of processing nodes or servers. The network apparatus includes a content based message director (e.g., XML [i.e., Extensible Markup Language] director) to route or direct messages received from the network to

one of the processing nodes based upon the application data . . . ." (Abstract, ll. 1-6.) More specifically, "[t]he application data is provided after the HTTP header, and in this example is provided as XML data." (Col. 6, ll. 4-6.)

Baskey "utilizes a modified SSL proxy server 40 to provide scalable secure communications between a client application 10 or 10' and a transaction server 50." (Col. 5, ll. 21-24.) "Furthermore, a single SSL proxy server 40 may have persistent secure connections to more than one transaction server 50. In such a case the routing function would also determine the destination of a communication from a client and route the communication to the corresponding persistent secure connection." (Col. 6, ll. 30-35.) The latter reference's "format function may be incorporated into a protocol stack between the Secure Socket Layer and the application layer of the protocol stack." (Col. 10, ll. 9-11.)

ANALYSIS

Hankinson teaches that a server may handle encryption/decryption for SSL transactions. It is uncontested that "[t]here is no teaching or suggestion that [the reference's] SSL is supported in a manner that is different from the prior art, i.e., where application data is reassembled via the application layer for decryption (see Figure 2B of Appellants' Background)." (Appeal Br. 17.) Even if Toporek's teaching of bypassing an application layer of a network stack was combined with the teachings of Hankinson, therefore, we agree with the Appellants that "[t]here is no teaching in Hankinson in view of Toporek as to how a device could decrypt secure data using a process that

bypasses the application layer." (*Id.* at 18.) To relocate the encryption/decryption of Hankinson to a lower layer in the stack would require impermissible hindsight, i.e., use of the claimed invention as an instruction manual or template to piece together the teachings of the prior art so that the claimed invention is rendered obvious.

For its part, Abjanic provides an XML director to route or direct messages received from a network to a processing node based upon application data. The application data are provided after an HTTP header as XML data. It is uncontested that "HTTP headers and XML data are only available at the application layer." (Appeal Br. 21.) We agree with the Appellants that "a modification so as to bypass the application layer, as proposed by the Examiner, would likely render the Abjanic device inoperable or defeat its essential purpose since no XML data would be identified." (*Id.* at 21-22.)

For its part, Baskey discloses a modified SSL proxy server that provides secure communications between a client application and a plurality of transaction servers. In contrast to Hankinson and Abjanic, Baskey teaches incorporating its functions into a protocol stack below the application layer. It also teaches an SSL layer separate from the application layer. Therefore, the reference would have suggested a combination with Toporek's teaching of bypassing an application layer of a network stack. Such a modification, moreover, would not likely render the SSL proxy server inoperable or defeat its essential purpose.

CONCLUSION

Based on the aforementioned facts and analysis, we conclude that the Appellants have shown error in the Examiner's combining of teachings from Toporek with those of Hankinson and Abjanic. We also conclude, however, that they have shown no error his combining of teachings from Toporek with those of Baskey.

DECISION

We reverse the rejection of claims 1-28 under 112, first paragraph, and the rejections of claims 1-7 12-15, and 17-24 under 103(a). In contrast, we affirm the rejection of claims 25-28 under 103(a).

No time for taking any action connected with this appeal may be extended under 37 C.F.R. § 1.136(a)(1). *See* 37 C.F.R. § 1.136(a)(1)(v).

AFFIRMED-IN-PART

Vsh

SHUMAKER & SIEFFERT, P.A
1625 RADIO DRIVE , SUITE 300
WOODBURY MN 55125